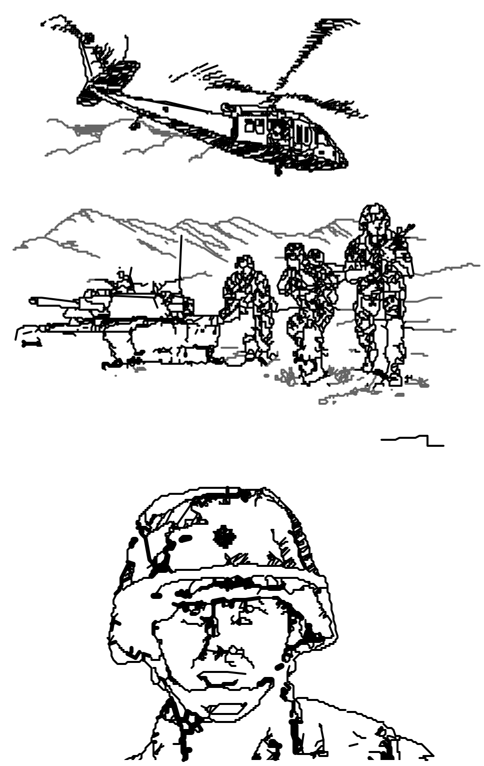
ARAT BULLETIN

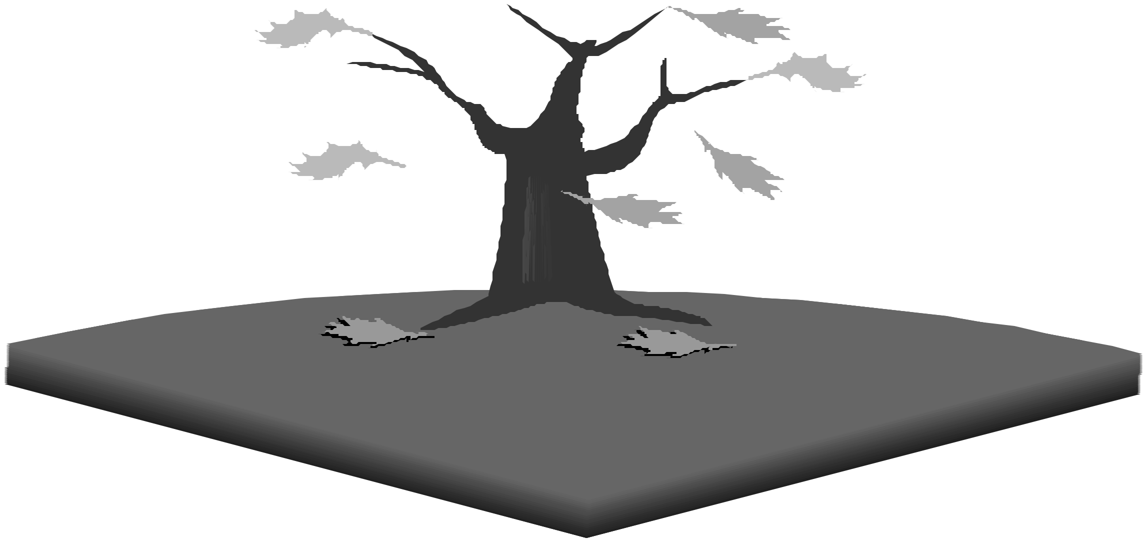
Published by ARAT-PO
Fort Monmouth, NJ 07703

Volume 3, Issue 3 **November 1996**

JOINT REPROGRAMMING EXERCISE PARTICIPATION BRAVE BYTE 96



What's Inside:



It's autumn and, like the weather, things are changing for the Communications-Electronics Command (CECOM), Software Engineering Directorate (SED), located at Fort Monmouth, New Jersey. CECOM is undergoing considerable restructuring which results in a significant amount of additional missions and resources in the information management area. Some of these changes impact directly on the SED.

Effective 1 Oct 96, SED transitioned to become the Software Engineering Center (SEC) (provisional). SEC consists of all assets and missions currently assigned to SED plus significant new assets and missions. These include those of the Information Systems Software Center (ISSC) which was part of the Information Systems Engineering Command (ISEC). In addition, the Industrial Logistics Systems Center (ILSC) and the Logistics Systems Software Center (LSSC) have been transferred to SEC. Operational control of the ILSC and LSSC transferred to CECOM on 1 Oct 96 from the Industrial Operations Command (IOC) and Missile Command (MICOM) respectively. Mr. Dennis Turner is designated as the Acting Director of the provisional SEC.

These decisions resulted from the Vice Chief of Staff, Army (VCSA)-directed information management functional area assessment, Assistant Secretary of the Army for Research, Development and Acquisition (ASARDA) decisions regarding the realignment of the Program Executive Office (PEO) structure, and other related decisions made by the commanding general of Army Material Command (AMC). They are intended to increase effectiveness in the engineering and acquisition of information-based weapons systems and capabilities for the Army while at the same time providing opportunities for increased efficiencies associated with the merging of these missions within CECOM.

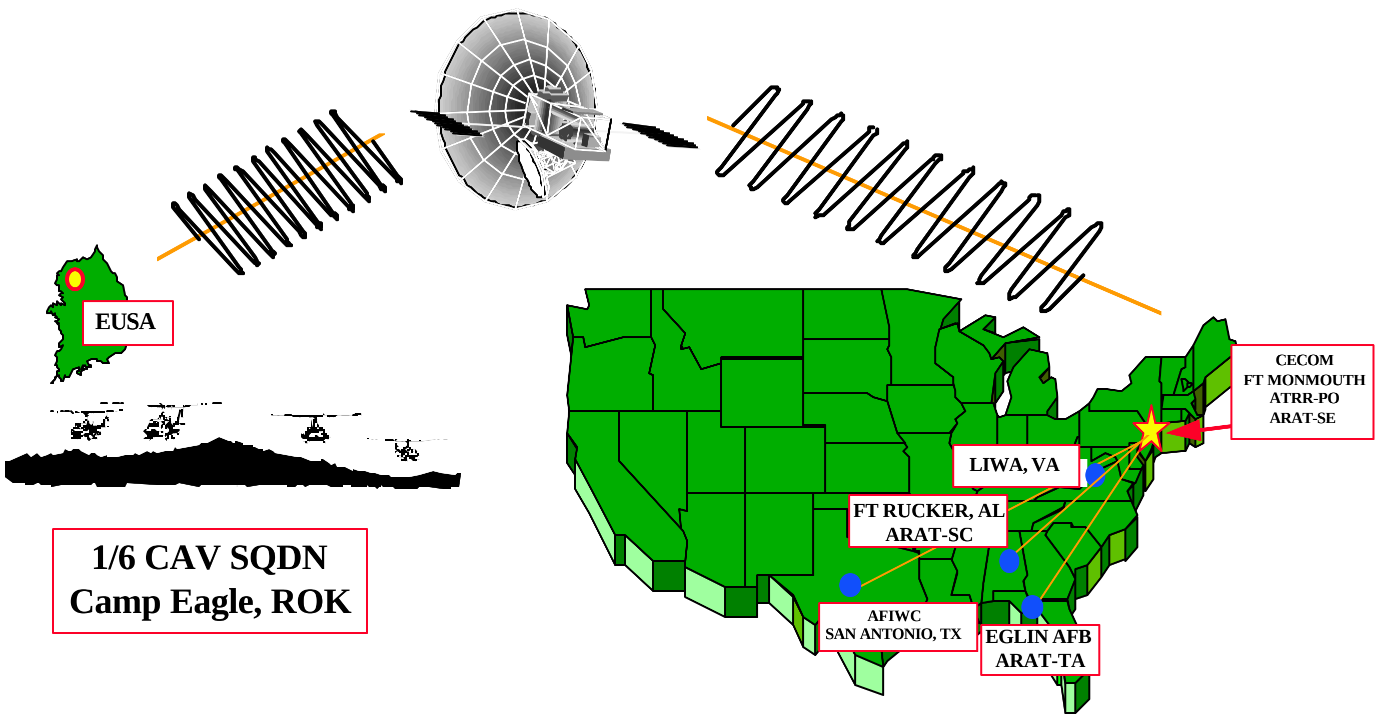
Note: Information in this article was extracted from a memorandum released by the office of Major General Gerard P. Brohm, CECOM Commanding Officer, dated 9/30/96.

BRAVE BYTE '96 AND ULCHI FOCUS LENS '96
A SUCCESS FOR ARMY REPROGRAMMING!

A primary objective of the Army Reprogramming Analysis Team Project Office (ARAT-PO) is to develop an infrastructure which supports rapid reprogramming of Army Target Sensing Systems (TSS). This effort involves periodic participation in major Army exercises to test the infrastructure. ARAT-PO and the Army Reprogramming Community recently participated in Exercise BRAVE BYTE 96 (BB96), conducted concurrently with the Joint Chief of Staff (JCS) Exercise ULCHI FOCUS LENS 96 (UFL96), in the Republic of Korea (ROK). The main objective of BB96 was to exercise, in a simulated scenario, the Army rapid reprogramming infrastructure and capabilities.

While exercising the infrastructure, BB96 also had these training objectives: assess the ability of the ARAT-TA, ARAT-SE, ARAT-SC and ARAT-PO to adequately staff and equip software support and reprogramming facilities; assess the timely and accurate flow of information between members of the software reprogramming community; assess the intelligence and reprogramming communities response to threat changes; evaluate the capability of the existing Multi-Service Electronic Combat Data Distribution System (MSECDDS); determine the effectiveness of signature libraries and flagging models; evaluate the decision process that will create and implement tactics, techniques, and procedures (TTP); evaluate the

(Continued Next Page)



Key Army reprogramming participants during BRAVE BYTE 96 are shown above.

reprogramming community's actions and training as it pertains to software rapid reprogramming; and determine if the scripted TACELINT simulators, signal generators, and exercise intelligence collection are adequate to replicate new or changed emitters for the purpose of rapid reprogramming.

To support the exercises, the ARAT project expanded its communications and added redundancy through a World Wide Web (WWW) interface which enabled electronic file transfer of Mission Data Sets (MDS). Prior to the start of the exercises, the Electronic Warfare Officer (EWO) in Korea, CW4 Stephen Woods received equipment and training on Transmission Control Protocol/Internet Protocol (TCP/IP) access on the Secure IP Router Network (SIPRNET) using STU III dial-in connection to the ARAT Rapid Reprogramming Communications Infrastructure Laboratory (R2CIL). This Point to Point Protocol (PPP) connection gave the location in Korea access to any service host, including the MSECDDS at Eglin Air Force Base, Florida. The WWW interface created by the ARAT Project Office allowed the EWOs access via INTERLINK-S, the SIPRNET web.

The ARAT-PO sent a representative to the ROK to observe and assess SIPRNET and MSECDDS communications connectivity, and the ability of EWOs from the 1-6 Cavalry Squadron, 17th Aviation Brigade, Camp Eagle, to gain full electronic access to updated AN/APR-39A (V)1 Mission Data Set (MDS) files and messages and reprogramming training objectives. Using the web browser interface, personnel in Korea could log into an account on MSECDDS to read email or download exercise files by file transfer protocol (ftp) simply through point and click of the mouse. Files on the R2CIL SIPRNET web server established a UFL page with direct password protected links to the Korea EWO to download exercise information expeditiously.

Key Army reprogramming community participants included ARAT-SE and ARAT-PO at Fort Monmouth, NJ; ARAT-TA at Eglin AFB, FL and Kelly AFB, TX; ARAT-SC at Fort Rucker, AL; and 1/6 Cavalry Squadron, Camp Eagle, Korea. In addition, the US Air Force at Eglin AFB provided analytical support. (show this on a map graphic)

During the course of the exercises, the ARAT community exercised the entire reprogramming process, from initial threat change to actual Radar Warning Receiver (RWR) reprogramming with outstanding results. This exercise demonstrated the capability for electronic transfer of data files into theater within a matter of minutes after completion. This is a major progression from past exercises where needed reprogramming data files were hand carried or mailed into theater, taking several days to weeks. Both exercises helped to highlight the considerable progress achieved in supporting rapid reprogramming operations within the Army Aviation community. It also focused attention on areas which still need improvement such as communications. BB96 served to highlight these problems, some of a general nature and some unique to the Korean theater of operations

The ultimate goal of all this activity is to provide a wider variety of user-interfaces that better meet the various needs of the reprogramming community. This effort by the project office, using state of the art automation for communications has provided the warfighter the reprogramming data files necessary to sustain his battlefield systems and thus maintain the critical technological edge. Further information can be obtained by contacting the ARAT Project Office. POC is Mr. Joseph Ingrao, DSN: 992-1337/Comm. (908) 532-1337.

MLVs were used to provide near real-time reprogramming to Aviation units.

SCREAMIN' EAGLES GET REPROGRAMMING SUPPORT!

The 101st Aviation Brigade, part of the 101st Airborne Division (Air Assault - AASLT), Fort Campbell, Kentucky, was visited recently by representatives from an ARAT training team. The team trained unit personnel on the availability, understanding, use, maintenance, and reprogrammability of the AN/APR-39A(V)1 Radar Signal Detecting Set (RSDS) installed on the many different types of platforms within the Brigade. PM-AEC had received a number of reports concerning problems understanding the operation of the RSDS.

Colonel Thomas Mathews, the 101st Aviation Brigade Commander, hosted an in-brief for the team. He emphasized that his unit is the "ready unit" for the division, subject to deployment at a moments notice. Thus, it is critical that all aviators and support troops understand RSDS operations and how to obtain correct Mission Data Sets (MDS). Over 100 members of the 101st Aviation, including aviators, maintenance, and intelligence personnel participated in the training.

Team members briefed many facets of RSDS operations. They provided detailed descriptions of how and why anomalies occur on the system - primarily through poor or nonexistent grounding/bonding straps. The team provided unclassified bulletin board system (BBS) phone numbers to allow direct access to information about their EW systems, maintenance, logistical and fielding status.

The team also briefed operational use of the RSDS. It discussed types of threats (by specific example) that the "box" could and could not cover. It stressed system limitations and capabilities to create better aircrew awareness with regards to maintainance and programming with the correct Operational Flight Program (OFP) and MDS. The team reviewed the status of all MDSs available to the US Army, again citing the importance of having the most current MDS loaded to increase detection and survivability. Basic radar parameters used by the system to discriminate signals were also reviewed. This allows the aviator to draw comparisons between threat and non-threat emitters -- even though some use the same type pulse characteristics, e.g., short to medium Pulse Repetition Intervals. This point was emphasized because ambiguities were being reported as misidentifications.

Threats loaded to the MDSs, symbology and the audio were covered, as these can and do vary depending upon the MDS loaded and mode selected on the RSDS control head. A short briefing was also given on the function of and support available from the ARAT-TA organization through its parent, the US Army Land Information Warfare Agency (LIWA). The team discussed the intermittent Background Built-in-Test (BBIT) anomaly- which appears as an "F" in the center of the IP1150A display. It emphasized that if this condition happens, the aircrew should press the 'test' button on the RSDS control head to determine if the "F" is indicative of a hardware failure. The test clears the "F" if the hardware is operational.

The day's final event involved the fielding of RSDS reprogramming kits furnished by the ARAT Project Office. Each of the nine Battalion EWOs was given the software package and an RSDS upload cable.

(Continued Next Page)

Screamin' Eagles (Continued)

A demonstration on the simplicity of accessing the Multi-Service Electronic Combat Bulletin Board System (MSECBBS), the downloading of an MDS to meet the EW and deploying requirements of the 101st, and the uploading of the MDS to the RSDS was effected with ease. Examples of the MDS kneeboard sheets and pertinent notes to correlate to the programmed MDS were also provided.

The visit proved highly beneficial for all participants. The changing threat environment, deployment challenges and a requirement to ‘play’ in the information age puts added pressure on the command structure and EWOs to ensure availability of the most current data for use in tactical and operational situations. Colonel Mathews felt that additional training would be required for his unit to ensure that all aviators, support personnel and maintainers presently in the field would receive this information.

Accordingly, coordination is ongoing to provide additional training to the 101st Aviation, with PM-AEC having the lead. Other units interested in receiving technical assistance visits to improve reprogramming capabilities should contact the ARAT-PO. POC is Mr. Joseph Ingrao, DSN: 992-1337/Comm: (908) 532-1337.

NOTE. The ARAT Team was composed of the following personnel: LTC Lovett - PM AEC; CW3 Gregg Dorough - PM AEC; Mr. John Riley, CECOM NVESD; Ms. Fanny Leung-Ng, CECOM SEC; and Mr. Pete McGrew, ARAT-TA.

ARMY FLAGGING: PROCESS IMPROVEMENT CONTINUES

“On a distant battlefield, an OH-58 scout helicopter skims above the tree tops looking for an artillery battery that pounded friendly infantry the night before. As the scout banks to circle behind a hill, a “U” appears at the top of the APR-39A(V)1 Radar Warning Receiver (RWR) display, a telltale sign of a possible air defense radar. A second and third “U” soon follow at the six o’clock position. The pilot knows he’s in a bad situation since he has several likely threat emitters illuminating him and no idea what they are. Back in the US, ELINT traffic continuously pours into the Army Reprogramming Analysis Team-Threat Analysis (ARAT-TA) Center. In the last 24 hours, more than 1,000 Tactical Electronic Intelligence (TACELINT) messages have been sent from the theater, including the intercepts from the AAA guns tracking the OH-58. The analysts at the ARAT-TA struggle to compare the ELINT intercepts with MISREPS from aviators who reported anomalies on their A(V)1 sets. The anomalies continue to accumulate, but a new mission data set for the scout helicopter is still several days away. ...”

This scenario was possible just one year ago, but no longer. Today, Army aviation enjoys the benefits of flagging as part of its rapid reprogramming support. Since late 1995, an ARAT engineer has resided at the Air Force Information Warfare Center (AFIWC) in San Antonio, Texas to provide dedicated reprogramming support for Army Target Sensing Systems (ATSS). While many have heard flagging defined as identifying signals whose parameters are outside expected or programmed limits, the practical value of flagging to ARAT-TA is that it reduces to a manageable level the number of signals needing analysis. During a contingency, thousands of TACELINT messages flow into the ARAT-TA daily. It is not possible to analyze that amount of traffic and make reprogramming decisions. The flagging function identifies out-of-limit signals and, thus eliminates 98 to 99% of the ELINT volume that the ARAT-TA must analyze. Instead of thousands of signals, the ARAT-TA now evaluates one or two dozen. That is a powerful capability!

(Continued Next Page)

Army Flagging (Continued)

To reduce the volume of ELINT traffic that is forwarded to ARAT-TA, flagging employs a substantial amount of automation. Typically, up to 10,000 signals per day in various formats must be evaluated to determine how each of these signals would be processed by radar signal detection sets (RSDS) and jammers. To accomplish this sizable task, signals are processed in several steps, with expert system technology employed throughout the process to minimize human intervention. ELINT intercepts arrive from the field in several formats. The first task for an automated system is to parse these messages into a single, consistent format. Of course, message traffic has been known to contain format errors. When the parser detects a message with a format error, it signals for help from an ELINT analyst. The analyst corrects the format and sends the message back into the system.

Before these signals are processed by the flagging models of the RSDS and jammers, one must know with high confidence what type of system emitted the signal. Signal IDs are not always correct in ELINT reports and sometimes the signals are not identified at all. Correct identification of signals is the bread and butter of flagging. When threat emitters change their operating parameters, the signal may not be recognizable any more and is reported without identification. It is the task of flagging to use all available means, parametric, geographic, or other intelligence sources such as imagery or COMINT, to correctly identify the emitter of an unknown signal. These are the signals that will most likely cause problems for Army aviators. The system that identifies these signals is called Electronic Warfare Flagging Analysis Expert System (EWFAES). It was developed by the Air Force to reduce the workload on ELINT analysts when identifying unknown emitters. Some signals may still require manual analysis in instances where analysis by the expert system does not produce an ID. However, those numbers are a small fraction of those entering the system.

After all the signals are correctly identified, each is processed through software simulations, or models, of various EW systems. Those signals that are not processed correctly by the models are flagged for further analysis by the reprogramming center. That is where the term flagging originates. The software models are designed by the flagging engineer to simulate the identification algorithms of the EW system. The signals are processed by the model using the mission data sets (MDS) that are applicable. The model response to the signal is evaluated, and if the response is correct, the model determines why it is incorrect and which parameter is outside limits. The output of the flagging model is reviewed by an ELINT analyst who ensures the signal is valid and also by the flagging engineer who looks for problems with the model itself. After that final quality control (QC), the flag is reported to ARAT-TA.

ARAT-TA uses flagging reports to determine if reprogramming actions are necessary. One of the first actions taken is to send flagged signal parametrics to CECOM SEC for additional analysis. The signal is programmed into a signal generator and transmitted into an actual APR-39A(V) 1 system. If the A (V) 1 produces unacceptable results as well, ARAT-TA must determine what, if any, actions are necessary to address the threat. Reprogramming is not always necessary or the best solution. If the numbers of radars emitting signals outside normal limits are small and in one location, a call for artillery support may be a better solution. Ordering up a barrage of 155mm HE rounds is easier than reprogramming and has a more permanent effect. In other cases in which reprogramming is necessary, the flagging reports provide ARAT-TA concise data on signal parameter limits. ARAT-TA uses this data to build new mission data sets which incorporate the new operating parameters of the threat radars.

Since Army flagging was established, ARAT-TA's ability to support soldiers has improved substantially. Shortly after its establishment, the flagging facility rebuilt a flagging model of the APR-

(Continued Next Page)

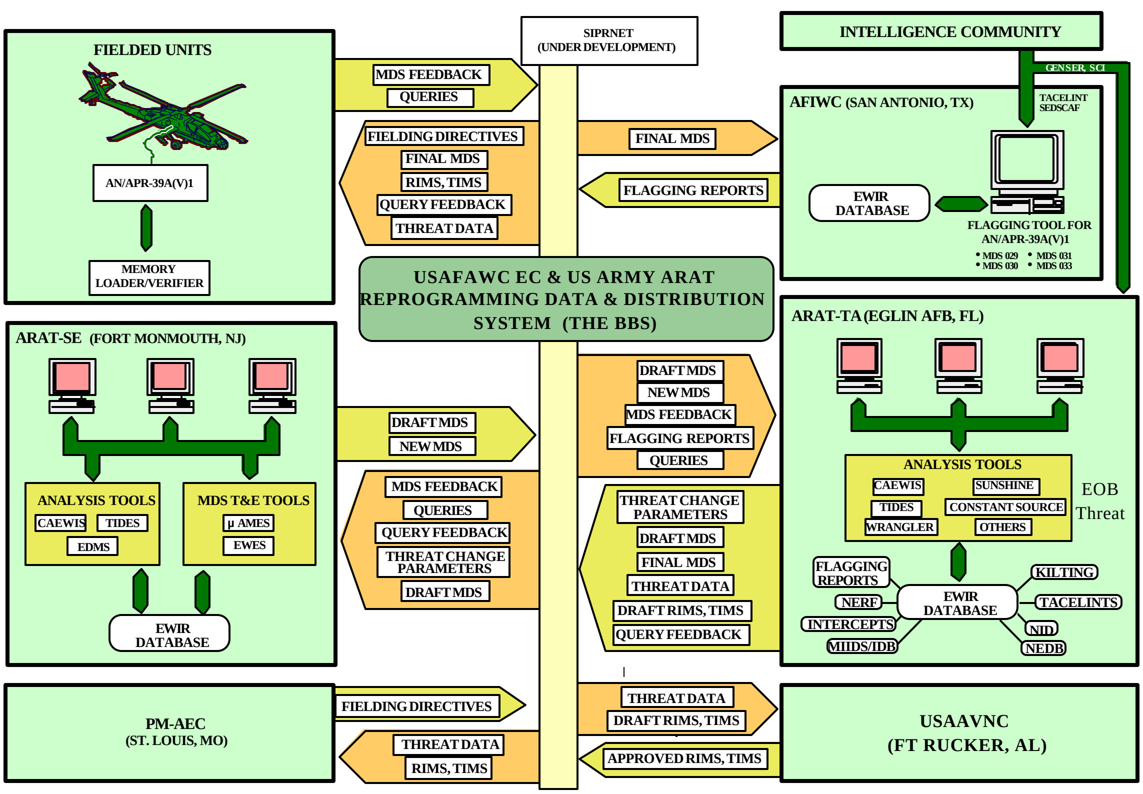
Army Flagging (Continued)

39A(V) 1 to simulate OFP 20.9 and 23.9 with higher fidelity. This first step insured the quality of the flagging reports on which ARAT-TA depends. The models currently support four Army and two Air Force MDS, and more Army sets are being developed. After a new MDS is released, the first flagging reports typically are forwarded to ARAT-TA within 48 hours. Flagging's value was clearly proven during Exercise BRAVE BYTE 96, the annual Army reprogramming exercise. Previous BRAVE BYTE exercises had limited success because the huge volume of ELINT traffic overwhelmed the ARAT-TA. With the benefits of flagging, ARAT processed more than 13,700 ELINT reports, identified all scripted parametric changes, produced and distributed a new MDS in response to the changed parameters, and installed the new mission data on the flagging model to begin the next iteration.

So how does this benefit the aviator? The addition of flagging to the reprogramming process has eliminated the potential log jam of ELINT traffic that could delay new mission data from getting into aircraft. It allows ARAT-TA to concentrate on programming the A (V) 1 to identify the signals that are causing the aviator problems over the battlefield. And most important, it ensures that tomorrow his A (V) 1 will correctly identify the "U" he saw yesterday. POC is Mr. Norm Svarrer, DSN: 872-8899.

ARAT PROCESS EXAMPLE

AN/APR-39A(V)1



Flagging performs a key role in the reprogramming process

MASINT

First in a series

Measurements and Signals Intelligence (MASINT) describes intelligence collection of information which characterizes equipment operation or performance not related to Signals Intelligence (SIGINT) or Electronic Intelligence (ELINT). ARAT has supported the development and fielding of MASINT systems since 1991. Some Army Target Sensing Systems (ATSS) already exist which exploit MASINT, with more in advanced development. As such, MASINT is becoming a major area of focus for the Army Reprogramming Analysis Team (ARAT).

The following Table provides a representative example of the different types of MASINT information collected on vehicles, aircraft, missiles and support equipment.

DATA	COMMENTS
Thermal Infrared (IR) Heat Imaging	Where are the hot spots and how does the target look when in operation
Near IR Imaging	Just past visible light; used by night vision goggles; camouflage detection and use in night operations
Acoustic Signatures	What does the system sound like, or where is a target such as a sniper
Seismic Data	How much does the ground shake when the target roles past
Imaging Radar Data	Seeing through smoke, haze, foliage, and even water to try to detect and identify a target
Laser Imaging and Detection	Use of laser imaging systems for target and chemical/biological agent detection; detection and classification of emitters
Dimension and Feature Profiling	Deriving measurements on dimensions, weight, capacity, color, etc. to support modeling, simulation and algorithm development

Within the Department of Defense (DoD), the Defense Intelligence Agency (DIA) provides central coordination for MASINT collection efforts. Each service, in turn, has a primary command or staff activity to develop requirements and coordinate MASINT effort. Army responsibility resides with the Intelligence and Security Command (INSCOM). Army weapons systems programs that require MASINT information to support system design or operation submit requests through INSCOM for data collection and processing.

MASINT collection and processing is performed primarily by the Scientific and Technical Intelligence (S&TI) community to support research and development (R&D) programs. Every S&TI center has some involvement in MASINT collection or production which reflects that center's overall mission (National Ground Intelligence Center [NGIC] does work on armored vehicles, artillery, etc.) Service R&D centers such as the Communications-Electronics Command (CECOM) Research, Development and Engineering Center (RDEC), Night Vision and Electronic Systems (NVES) laboratory, are also involved in the collection and processing of MASINT.

Until recently, MASINT information wasn't managed centrally. Data was collected against service specific requirements, often supporting classified development efforts. As a result, information was hard to find or retrieve at a later date. In 1990, the Army started a MASINT data management effort intended to capture and provide MASINT information in a consolidated manner. This is similar to that available to the SIGINT and ELINT communities in the Electronic Warfare Integrated Reprogramming (EWIR), Kilting and Non-Communications Systems Data Bases (NCSDB). This effort evolved into a DoD-wide initiative managed by NGIC, called the National Target Signature Data System (NTSDS).

(Continued Next Page)

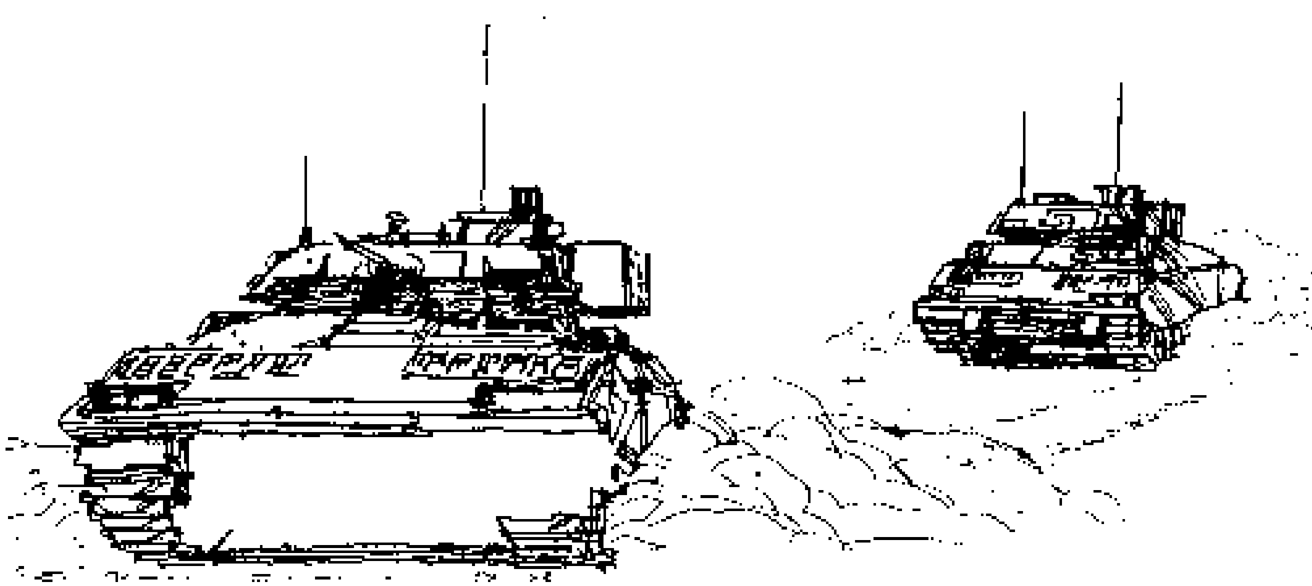
MASINT (Continued)

NTSDS is coming on line at the S&TI centers and service R&D activities. Commands can now access some MASINT data (primarily EO/IR images and measurements information) through the Secure Internet Protocol Network (SIPRNET), using web browsing software. Commands which require to access more detailed information must obtain approval from NGIC.

The R&D support emphasis that has characterized past MASINT collection and processing is shifting with the fielding of modern weapons systems. Some examples include laser detection and warning systems (AN/AVR-2/2A); Synthetic Aperture Imaging Radars (Airborne Reconnaissance low [ARL], Joint STARS); Millimeter Wave (MMW) target detection and classification systems (Apache Longbow); missile launch detection and warning systems (suite of Integrated IR Countermeasures [SIIRCM] and others); and target acquisition and engagement systems (Brilliant Anti-Tank [BAT], STINGER). As these systems are fielded, their capability must be continuously compared to the operational environment to ensure that they can perform their detection, acquisition, classification and engagement missions.

Few MASINT systems fielded prior to 1991 used embedded libraries, signatures or templates to perform autonomous detection, classification, tracking or engagement functions. This has changed markedly over the past five years, with the fielding of new aviation and fire support weapons. In the next few years, Army aviation will become more lethal with fielding of Apache Longbow, and more mission capable in all threat environments with SIIRCM and other systems.

The ARAT Threat Analysis (ARAT-TA), co-located with the US Air Force Air Warfare Center at Eglin AFB, Florida, has personnel assigned full time to MASINT issues. ARAT-TA is now available to answer questions on the programming and capabilities of MASINT systems, in addition to their traditional support for ELINT systems. ARAT-TA has also recently been staffed to provide support for SIGINT systems as well. Software programming updates for ATSS that can be programmed at the unit or direct support maintenance level are being placed onto the joint service electronic bulletin board system (BBS). Organizations with MASINT data collection or availability questions are encouraged to forward them through their local intelligence staffs. Questions related to specific ATSS system programming or capability should be referred directly to ARAT-TA or the ARAT Project Office (ARAT-PO). POCs are Mr. Joseph Ingrao, DSN: 992-1337/ Mr. Norm Svarrer, DSN: 872-8899.



MASINT can be targeted against a variety of equipment and vehicles.